



U.S. Department of Justice

United States Attorney  
Southern District of New York

86 Chambers Street, 3rd Floor  
New York, New York 10007

July 18, 2013

**BY HAND**

The Honorable William H. Pauley  
United States District Judge  
Daniel Patrick Moynihan U.S. Courthouse  
500 Pearl Street  
New York, NY 10007-1312

Re: *ACLU et al. v. Clapper et al.*, 13 Civ. 03994 (WHP)

Dear Judge Pauley:

In accordance with Your Honor's rules of practice, we write respectfully in response to plaintiffs' July 2 letter requesting that the initial conference now scheduled for July 25 serve as a pre-motion conference in anticipation of a preliminary injunction motion. Defendants request that the same conference also serve as a pre-motion conference for a potential cross-motion to dismiss the complaint. For reasons detailed below, we request that defendants' initial briefing on these matters be due no earlier than September 16. We request that this letter be docketed.

**Background:** This case concerns a highly sensitive and, in many respects, still classified intelligence-collection program that is designed to assist the U.S. Government in discovering whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities, including persons and activities inside the United States. Under this program, the Federal Bureau of Investigation (FBI) obtains authorization from the Foreign Intelligence Surveillance Court ("FISA Court") to collect telephony metadata from certain telecommunications service providers. The National Security Agency (NSA), in turn, archives this information; queries the data, when strict standards are met, to detect communications between foreign terrorist organizations and their potential operatives located in the United States; and provides leads to the FBI or others in the Intelligence Community for counterterrorism purposes. This program, which fills an intelligence gap highlighted by the attacks of 9/11, has been repeatedly re-authorized by multiple judges of the FISA Court as lawful under § 215 of the USA Patriot Act, 50 U.S.C. § 1861 ("Section 215") and the Constitution. The program has contributed to the disruption of multiple potential terrorist attacks in the United States and abroad.

The FISA Court's orders strictly limit the nature of the data the Government can collect, and the extent to which the data can be reviewed. The Government is not allowed to listen to or record the contents of anyone's phone calls. The information acquired under the Court's orders does not include cell-site location data or the names, addresses or identities of the parties to any communication. It is limited to telephony metadata, such as originating and terminating telephone numbers and the date, time, and duration of each call. Additionally, the Government is prohibited by the FISA Court's orders from indiscriminately sifting through the data. The data-

base may only be queried for intelligence purposes by NSA analysts where there is a reasonable, articulable suspicion (“RAS”), based on specific facts, that the query term, or “identifier” (e.g., a phone number), is associated with a specific foreign terrorist organization previously identified to and approved by the Court. Consequently, only a very small fraction of the records acquired under this program is ever reviewed by intelligence analysts. In 2012, for example, fewer than 300 unique identifiers were authorized for query under the RAS standard. Compliance with restrictions on the telephony metadata collection program is overseen by the Department of Justice as well as the Intelligence Community and is subject to regular FISA Court review. Furthermore, Congressional intelligence committees are regularly briefed on the program. Thus, the program has been approved and is rigorously overseen by all three branches of the Government.

**Discussion:** Plaintiffs allege that this court-sanctioned metadata program is unauthorized by Section 215, and violates the First and Fourth Amendments. They request a preliminary injunction barring the Government from querying the database “using any phone number or other identifier associated with [them],” and, as an apparent safeguard against such queries, “directing the [G]overnment to quarantine all of [their] telephony metadata,” assuming any have been collected. In effect, they ask this Court to overrule the order of a coordinate Article III Court, *see In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 486 (F.I.S.C. 2007); for the purpose of interfering with a judicially approved and overseen intelligence program that plays an important role in the Government’s overall strategy to protect the American people from terrorist threats. The requested injunction is irreconcilable with the public interest, and should be denied.

Plaintiffs here seek a mandatory injunction that alters rather than preserves the status quo, and so must make an even more compelling demonstration of an entitlement to preliminary relief than is normally required. *Cacchillo v. Insmid, Inc.*, 638 F.3d 401, 406 (2d Cir. 2011). Plaintiffs cannot carry that burden, because they fail to satisfy “the single most important prerequisite for the issuance of a preliminary injunction,” a showing of irreparable harm “that is neither remote nor speculative, but actual and imminent.” *Grand River Enter. Six Nations, Ltd. v. Pryor*, 481 F.3d 60, 66 (2d Cir. 2007). Plaintiffs cannot meet this essential requirement, even assuming their metadata have been or will be collected, because it is no more than speculation that their metadata have been or ever will be among the very small percentage of the records in the database that are ever reviewed. They neither allege nor point to any basis on which to conclude that any identifier of theirs is among the small number authorized for queries under the RAS standard. *See* Complaint, ¶¶ 25-27. Indeed, the chances that their metadata will be used or reviewed in a query are so speculative that they lack Article III standing to seek the injunctive relief requested in their July 2 letter. *See Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1146-50 (2013).

Moreover, plaintiffs cannot establish likelihood of success on the merits, and in fact, for reasons including but not necessarily limited to those discussed below, their complaint should be dismissed for failure to state a claim “that plausibly suggest[s] an entitlement to relief.” *Ashcroft v. Iqbal*, 556 U.S. 662, 681 (2009).

First, the challenged telephony metadata collection program is authorized by Section 215. Section 215 authorizes the FBI Director to apply to the FISA Court for an order for the production of “any tangible things” including “records” and “documents,” when there are “reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to protect against international terrorism.” 50 U.S.C. § 1861(a)(1), (b)(2)(A). Pursuant to the FISA Court’s orders, records can only be reviewed for intelligence purposes if there is reason-

able, articulable suspicion that the identifier used to query the database is associated with a specific foreign terrorist organization. The large volume of telephony metadata is relevant to FBI investigations into specific foreign terrorist organizations because to identify potential terrorist communications under this court-imposed query standard requires collecting and storing a large volume and high percentage of information about unrelated communications, to ensure that the much smaller subset of terrorist-related telephony metadata records are contained within the dataset. These data allow the Government to make connections related to terrorist activities over time and can assist counter-terrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities, including persons and activities inside the United States. If not collected and held by the Government, the metadata may not remain available for the period necessary for these national security purposes, because it need not be retained for that period by telecommunications service providers. Moreover, unless the data are aggregated, it may not be possible to identify telephony metadata records that cross different telecommunications networks. In short, because the telephony metadata must be available in bulk to allow the Government to identify the records of terrorist communications, there are “reasonable grounds to believe” that the data are relevant to authorized investigations to protect against international terrorism, as Section 215 requires, even though most of the records in the database are not associated with terrorist activity.

Second, the alleged metadata program is fully consistent with the Fourth Amendment. Most fundamentally, the program does not involve “searches” of plaintiffs’ persons or effects, because the collection of telephony metadata from the business records of a third-party telephone service provider, without collecting the contents of plaintiffs’ communications, implicates no “legitimate expectation of privacy” that is protected by the Constitution. *See Smith v. Maryland*, 442 U.S. 735, 739-42 (1979) (holding that use of a pen register installed at phone company’s central offices to record numbers dialed at petitioner’s home did not constitute a search, because petitioner had no “legitimate expectation of privacy” in the “numbers he dialed on his phone”). While plaintiffs suggest that the collection of the metadata “over long periods of time” compels a different result, the authority on which they rely, *United States v. Jones*, 132 S. Ct. 945 (2012), does not stand for this proposition. The Court’s holding in *Jones* turned on the Government’s physical intrusion on an individual’s property (his automobile) to attach a GPS tracking device, not on the duration of the surveillance. *See id.* at 949, 954. That concern is entirely absent here.

Finally, while plaintiffs contend that the Government’s acquisition of metadata chills First Amendment-protected activities, “surveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights.” *See, e.g., Gordon v. Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983); *see also Redd v. City of Enterprise*, 140 F.3d 1378, 1383-84 (11th Cir. 1998).

**Scheduling:** Although defendants’ response to the complaint is due on August 23, defendants request that they be permitted to file a combined motion to dismiss and opposition to the contemplated motion for preliminary injunction on a date no sooner than September 16. We make this request because the presentation of our arguments may be influenced by an ongoing, multi-agency declassification review that will determine whether and, if so, to what extent additional pertinent information about the metadata program may become available. The Government is endeavoring to complete this review by September 3. Given the potential importance of this process to the presentation and consideration of the parties’ motions, the Government requests that its brief on these motions be due no earlier than September 16.

STUART F. DELERY  
Acting Assistant Attorney General

JOSEPH H. HUNT  
Director

ANTHONY J. COPPOLINO  
Deputy Director

JAMES J. GILLIGAN  
Assistant Director

MARCIA BERMAN  
Senior Trial Counsel

BRYAN S. DEARINGER  
Trial Attorney

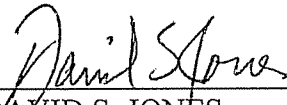
Civil Division, Federal Programs Branch  
U.S. Department of Justice  
20 Massachusetts Avenue, N.W.  
Washington, D.C. 20001  
(202) 514-3358

cc: Jameel Jaffer, Esq. (by email)  
Alex Abdo, Esq. (by email)  
Arthur N. Eisenberg (by email)  
Counsel for Plaintiffs

Respectfully,

PREET BHARARA  
United States Attorney

By:

  
\_\_\_\_\_  
DAVID S. JONES

TARA M. La MORTE

JOHN D. CLOPPER

CHRISTOPHER HARWOOD

Assistant United States Attorneys

Telephone: (212) 637-2739/2746/2716/2728

Facsimile: (212) 637-2730

david.jones6@usdoj.gov

tara.lamorte2@usdoj.gov

john.clopper@usdoj.gov

christopher.harwood@usdoj.gov